JOINT TECHNOLOGY COMMITTEE

BEYOND BITCOIN:
BLOCKCHAIN
2/23/18

“As our country and state face looming challenges in cybersecurity, we need to ensure that both Colorado and the nation are as prepared as possible for possible breeches. Our partners that are working to create the **National Cybersecurity Center (NCC)** will ensure that Colorado is the center for carrying out this mission.”

- CO Governor John Hickenlooper


"We're headed toward a cyber Pearl Harbor...." (Ret. Adm. James Stavridis)
ADM. JAMES STAVRIDIS | U.S. NAVY (RET.)
LIVE
MSNBC
ERE IS "FAR TOO MUCH TOLERANCE OF EXTREMISM" IN THE UK FOLLOWING THE
10:41 PM ET


NEIMAN-MARCUS


EQUIFAX


YAHOO!

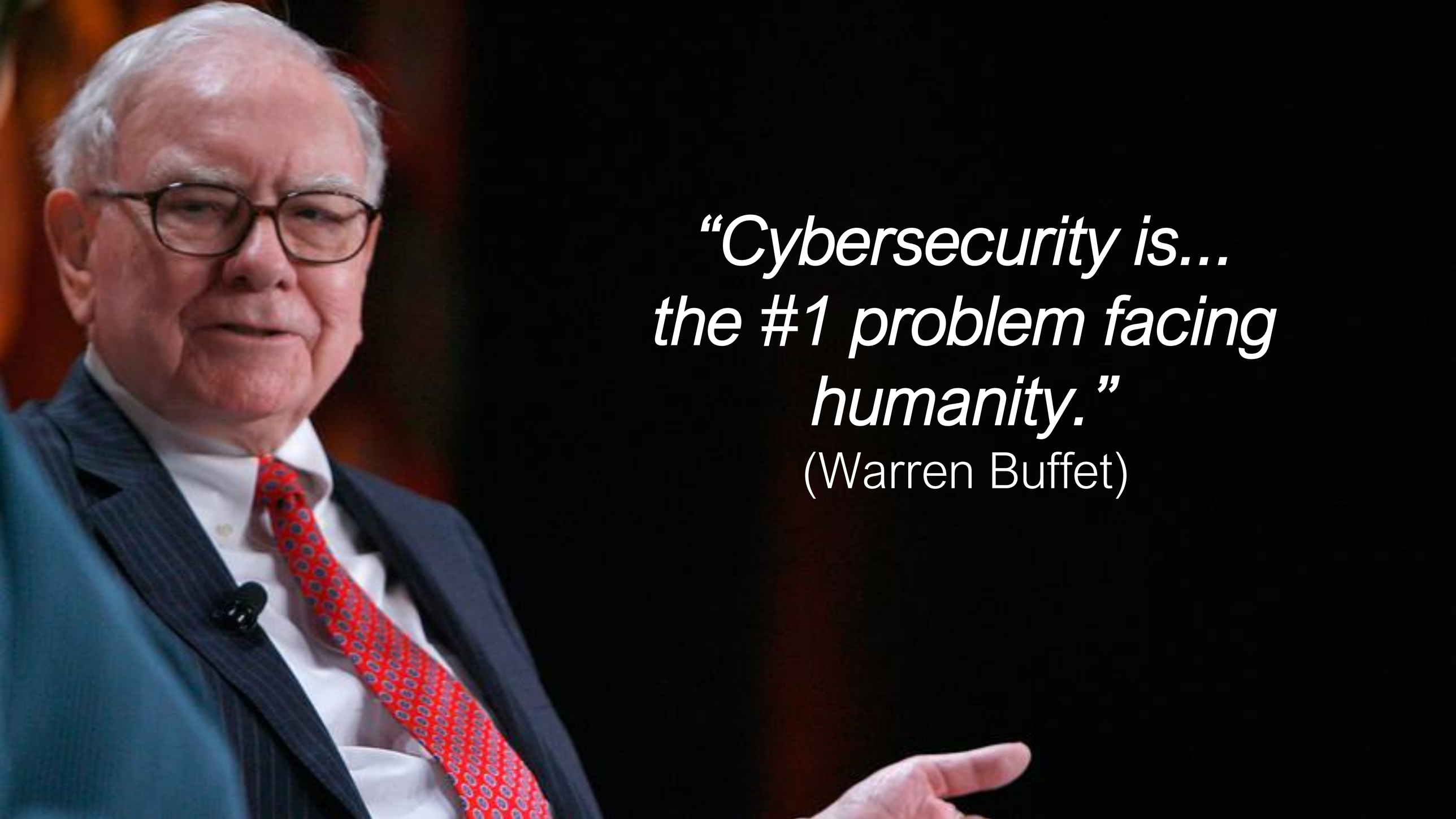
1 IN 3 HACKED IN 2017

THE FINANCIAL DAMAGES...

60% of small businesses close after a breach

$3 billion lost in the last three years through email scams

$6 trillion global cybercrime damages by 2021

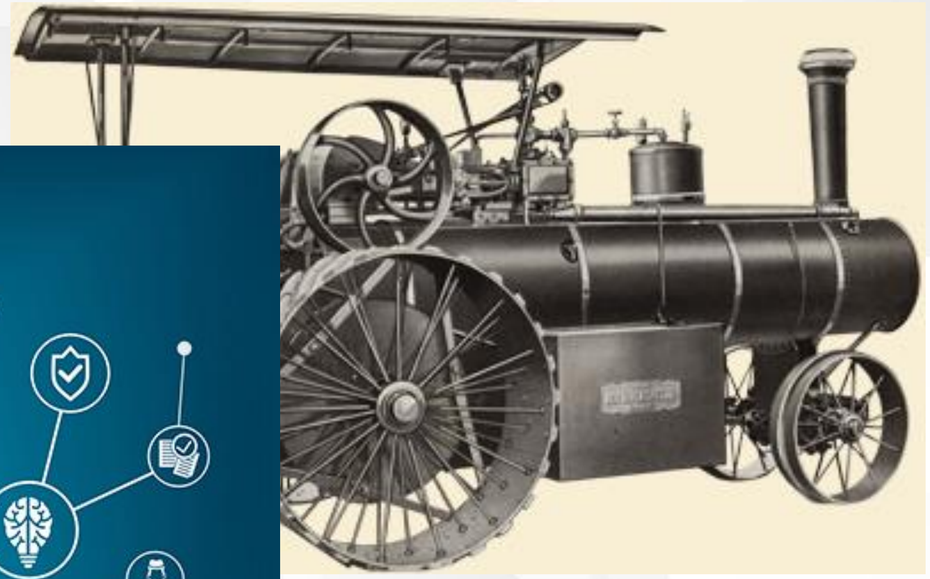

“Cybersecurity is… the #1 problem facing humanity.”
(Warren Buffet)

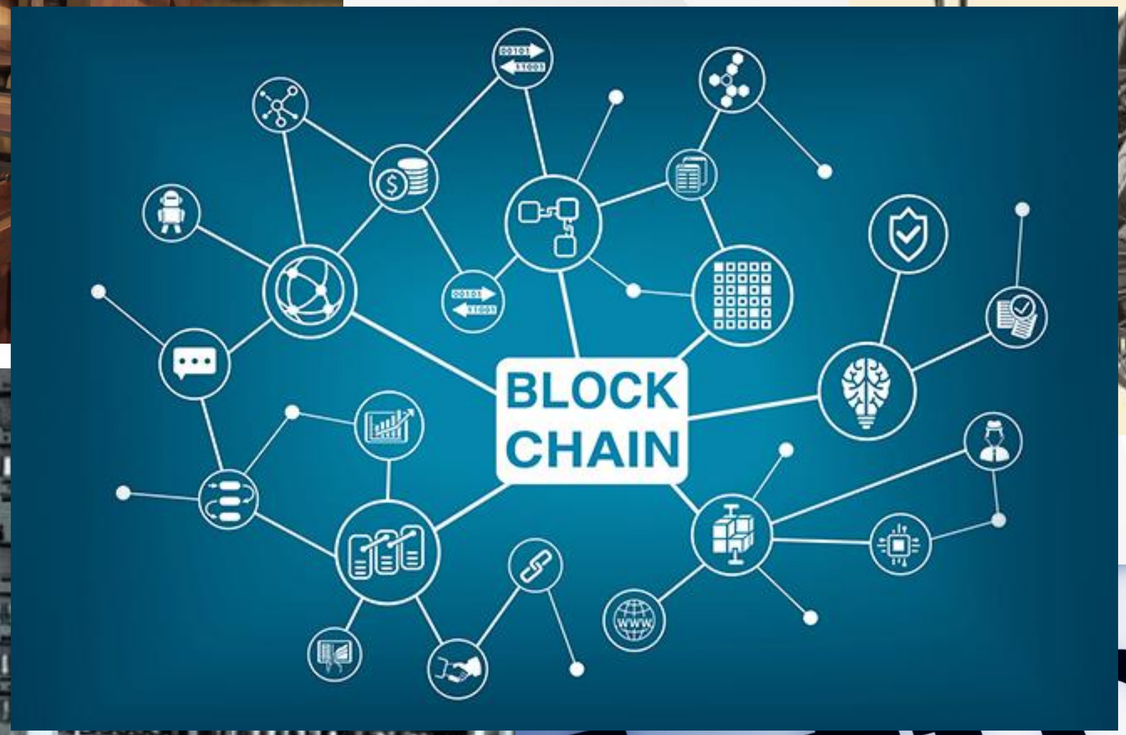
SPACE

HEALTHCARE


CYBERSECURITY...
HOPE FOR
THE FUTURE
NCC

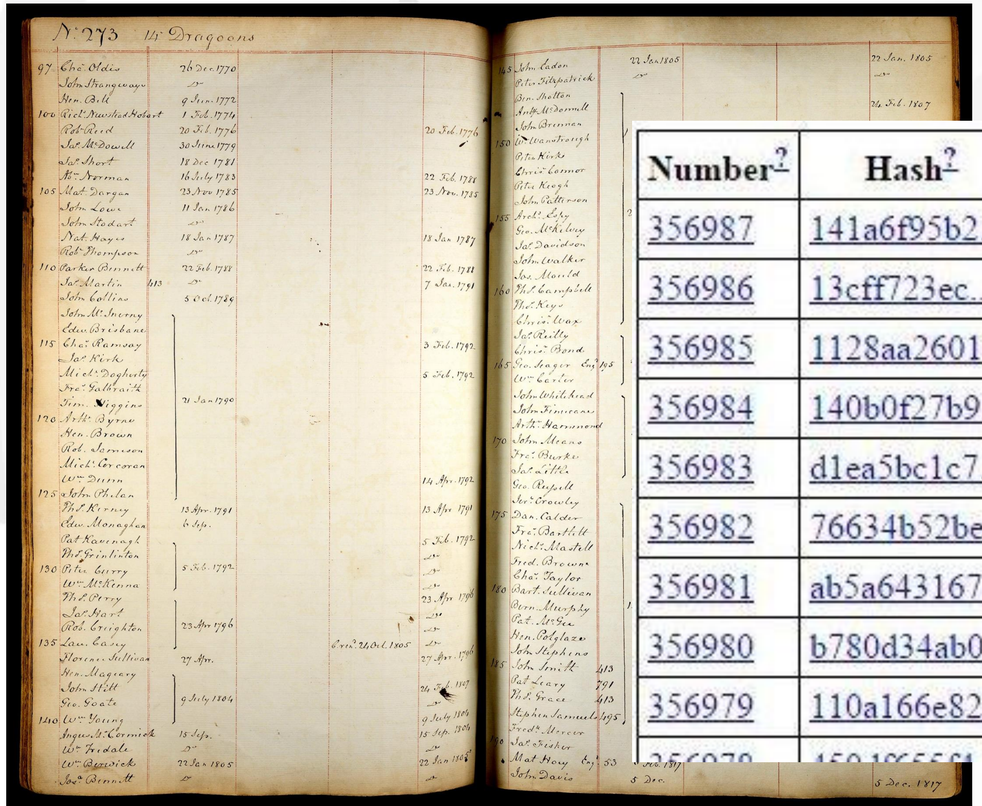
DEFINING MOMENTS



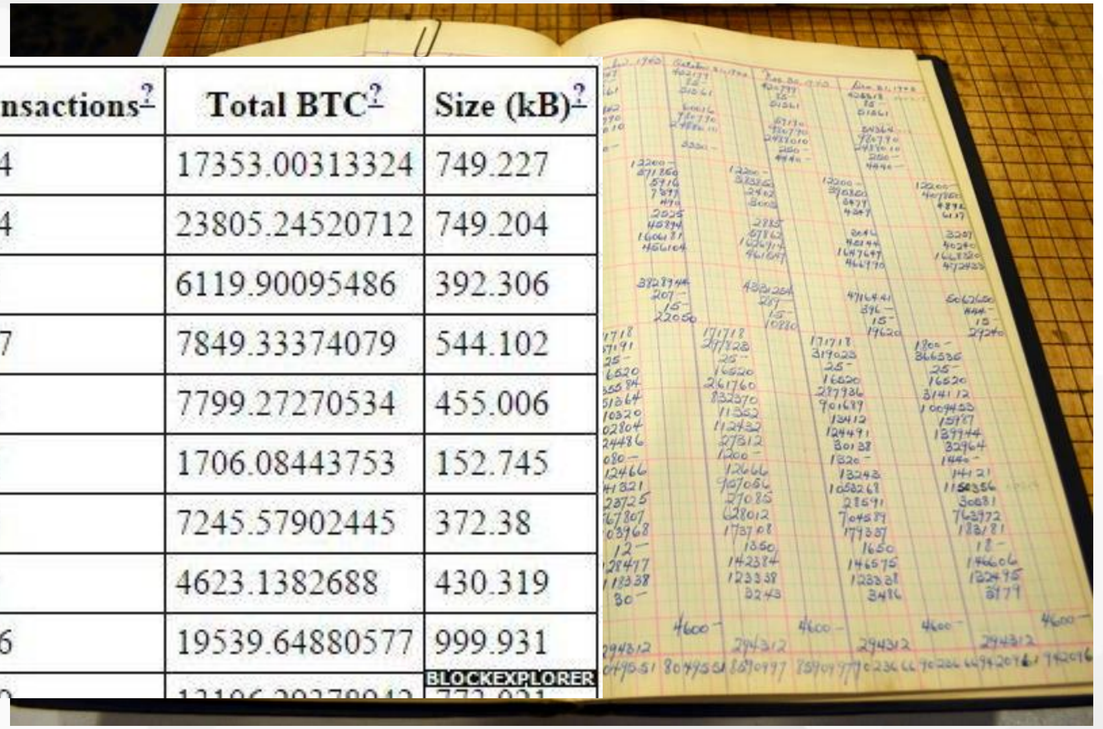


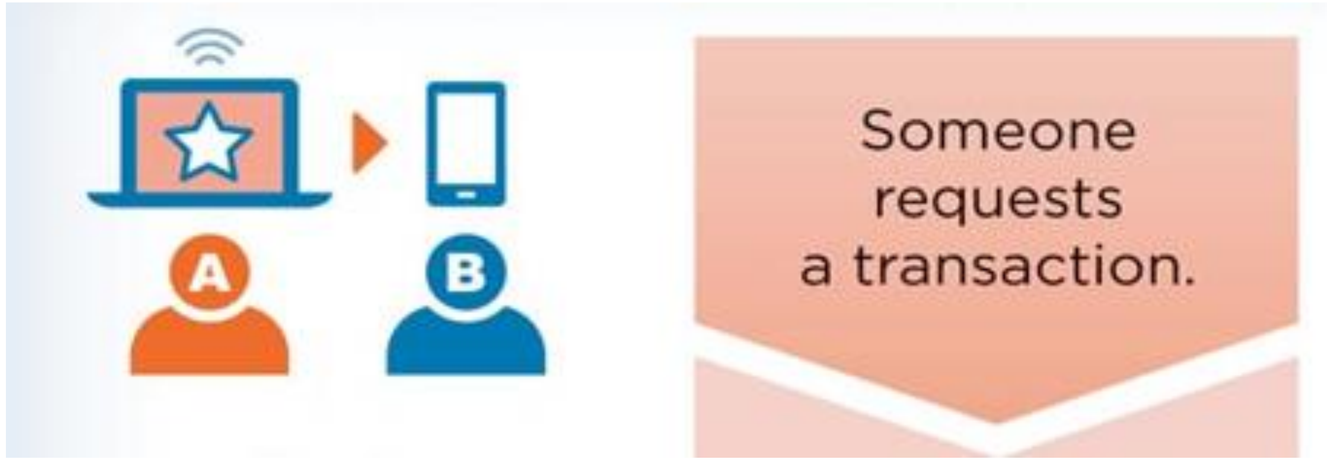
What is the Blockchain: DISTRIBUTED LEDGER TECHNOLOGY

A **blockchain** is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

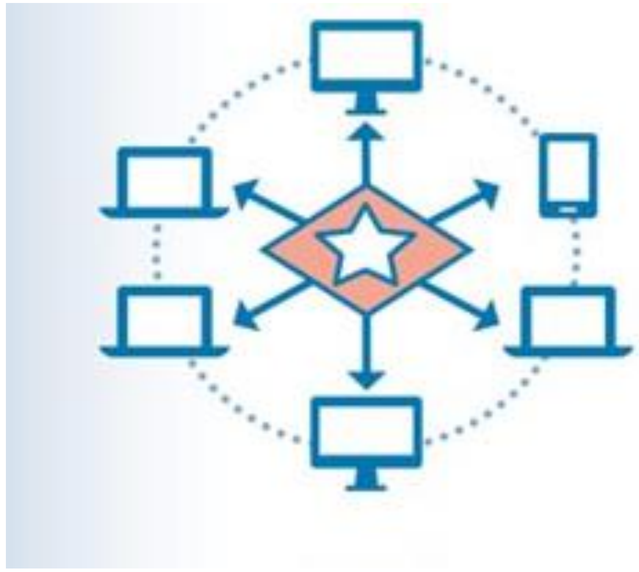


Number[?]	Hash[?]	Time[?]	Transactions[?]	Total BTC[?]	Size (kB)[?]
356987	141a6f95b2...	2015-05-18 13:28:14	1714	17353.00313324	749.227
356986	13cff723ec...	2015-05-18 13:11:53	2114	23805.24520712	749.204
356985	1128aa2601...	2015-05-18 12:27:49	594	6119.90095486	392.306
356984	140b0f27b9...	2015-05-18 12:20:14	1087	7849.33374079	544.102
356983	d1ea5bc1c7...	2015-05-18 12:08:01	830	7799.27270534	455.006
356982	76634b52be...	2015-05-18 11:58:42	221	1706.08443753	152.745
356981	ab5a643167...	2015-05-18 11:57:28	756	7245.57902445	372.38
356980	b780d34ab0...	2015-05-18 11:46:36	383	4623.1382688	430.319
356979	110a166e82...	2015-05-18 11:41:08	2276	19539.64880577	999.931



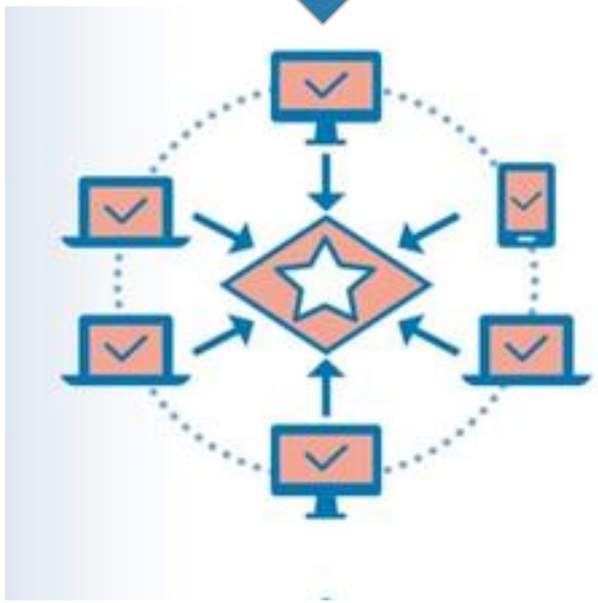


Someone requests a transaction.



The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.

Source: CSBJ

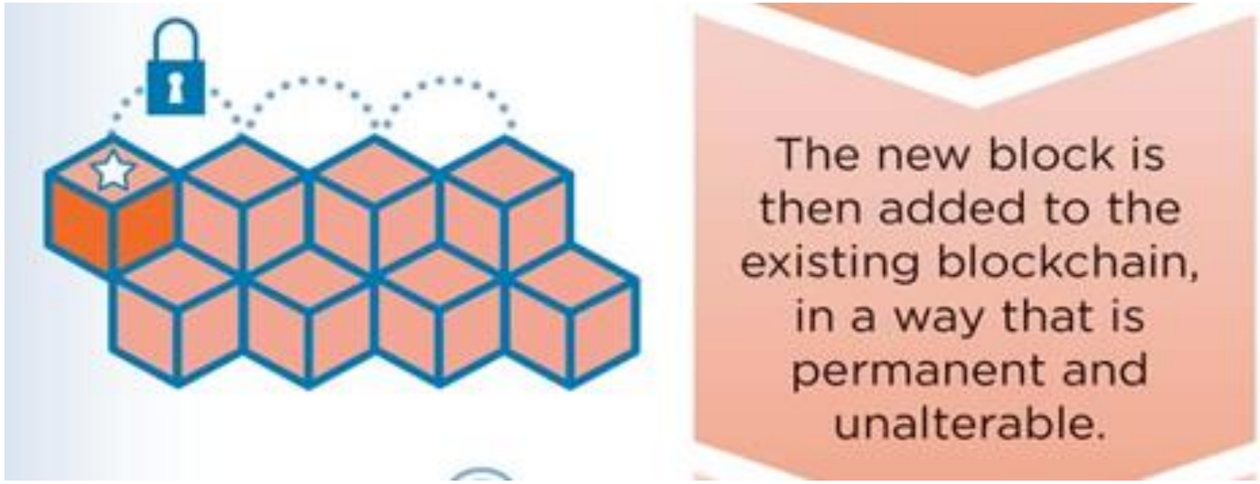


The network of nodes validates the transaction and the user's status using known algorithms.

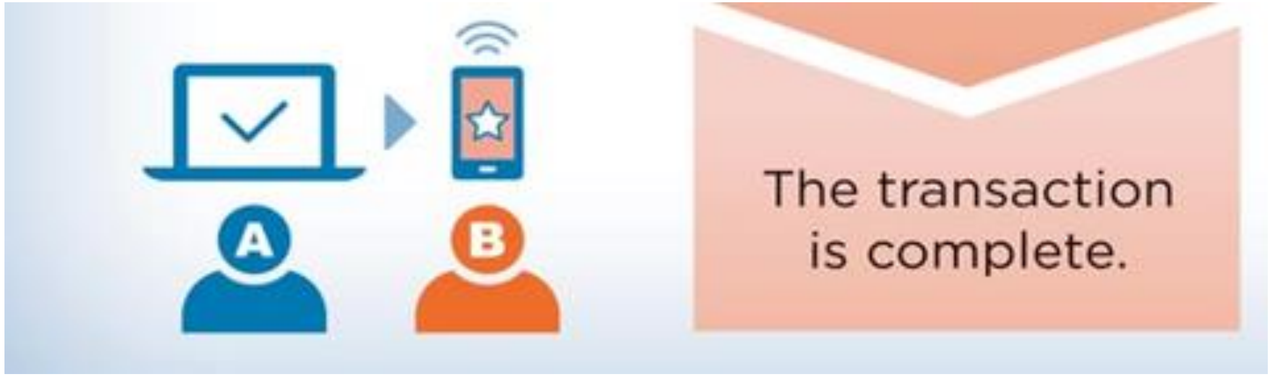
A verified transaction can involve cryptocurrency, contracts, records or other information.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

Source: CSBJ



The new block is then added to the existing blockchain, in a way that is permanent and unalterable.



The transaction is complete.

Source: CSBJ

HOW ARE TRANSACTIONS VALIDATED?

Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

Miner

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

Validator

WHAT IS THE BLOCKCHAIN?

Technical solution to provide TRUSTWORTHY transactions

- *Solves the digital "double spending" problem*
- *Today trust intermediaries (like banks) are used by centralizing copy of the transactions ledger*
- *How we store transactions – today can be tampered with*
- *This ledger is immutable – cannot be tampered with*
- *Networked computing power – all the nodes (computers) keep a copy of the ledger – no single point of failure*
- *Confidential yet transparent*
- *Transactions on the ledger are trusted because they are "validated" (via "proof of work" mining or "proof of stake")*

HISTORY OF BLOCKCHAIN

- *First application of Blockchain was Bitcoin*
- *Conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto*
- *Implemented in 2009 as a core component of Bitcoin (**BTC**)*
- *Ethereum (platform for building blockchain applications) was proposed in 2013 by Vitalik Buterin*
- *Ethereum platform went live in 2015*
- *Enterprise Ethereum Alliance (EEA) – Microsoft, Intel, JP Morgan, Deloitte, Cisco*

ETH DENVER – Largest Blockchain Hackathon in the World

ETHDENVER
HACKATHON+WORKSHOPS

Colorado – The Epicenter of Blockchain

WHAT ARE CRYPTOCURRENCIES?

- *First "Use Case" of Blockchain of financial transactions that are "peer-to-peer"*
- *Utility token vs Equity/Security token (Bitcoin – Digital Gold; Eth – Utility) - HB18-1220 includes all cryptocurrencies to be regulated under the "Money Transmitters Act" – would have unintended consequences*

CHALLENGES OF BLOCKCHAIN

- *Speed*
- *Scalability – Bitcoin 7 transactions/sec; Ethereum 20 transactions/sec; Visa 20,000 transactions/sec*
- *Transaction Fees (‘17 median Bitcoin $23; Ethereum $0.33)*
- *Energy (Proof of Work)*
- *New technology (familiarity and difficulty of use)*
- *Uncertainty of governance & regulation*

086: EXPLORE USE CASES OF BLOCKCHAIN

- *DORA Professional Licenses*
- *Real Estate Transactions (Deeds, etc)*
- *Secretary of State Business Records*
- *Integrity of Human Services Records (working to educate county agencies)*
- *Integrity of Elections*

A DEMOCRACY AT RISK

- *Proof that Russians interfered in the US elections*
- *Computers & emails have been hacked from both parties*
- *In a hacking competition, voting machines were easily hacked*

AHEAD

REGISTRATION

BLOCKCHAIN & ELECTIONS

Amber McReynolds
Denver Elections

Sarah Johnson
COS City Clerk


Vote
from
Absentee


RUNOFF
ELECTION


VOTING
Please Turn off
All Electronic
Devices Prior to
Entering The
Voting
Enclosure.

Reuters

ECONOMIC IMPLICATIONS

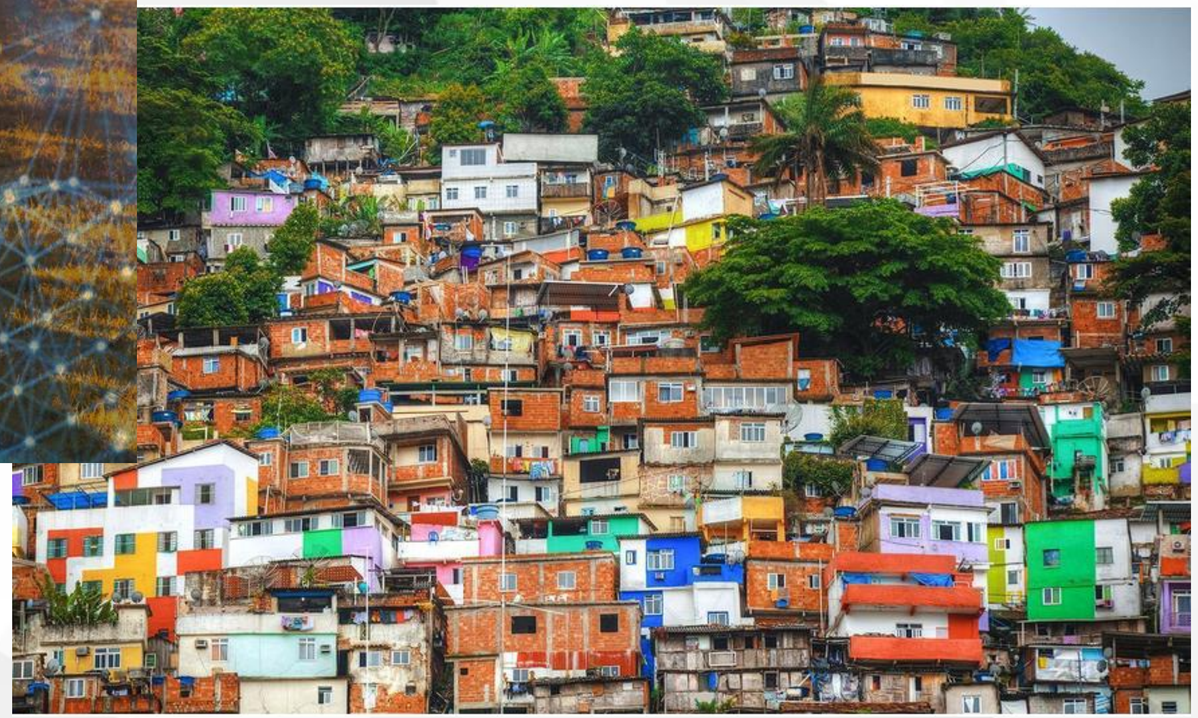
SUPPLY CHAINS

BANKING

SOCIAL IMPLICATIONS OF THE BLOCKCHAIN

IDENTITY

DISADVANTAGED



“Those who are crazy enough to think they can change the world usually do.”

(Steve Jobs)

DIGITAL WALLETS & KEYS

"Put very simply, cryptocurrency is represented by an entry in the blockchain associated to a public key.
In order to move currency around, exchange it, make a purchase with it, or convert it back to FIAT money, your private key is required to unlock it.

Typically, your private key is stored within your wallet.
If you lose your private key, your cryptocurrency is lost. This is why it is very important to consider how your private keys are stored." – HOBO with a Laptop

e3b3210ef2cace52e6a565bc97ddcd4a56310c1c1d33bca3f0b1478f0a67414e

0x62B4a242E4974875B500388432354376ABa786F2

ENS name: vancebrown.eth

Mnemonic Phrase: lamp rock gym paper check computer light sick money tree ash horse

SOCIAL IMPLICATIONS OF THE BLOCKCHAIN

- *Disadvantaged Communities*

https://www.google.com/amp/s/www.engadget.com/amp/2016/11/28/how-cryptocurrencies-will-help-the-poorest-people-in-the-world/

- *Supply Chain*

https://hackernoon.com/food-you-trust-how-blockchain-will-reinvent-the-supply-chain-1d6ae601ae53

- *Decentralized Digital Identities – especially for refugees and immigrants*

https://www.forbes.com/sites/laurashin/2017/06/22/the-identity-solution/#dbc3efa72ed0


CYBERSECURITY...
HOPE FOR
THE FUTURE
NCC